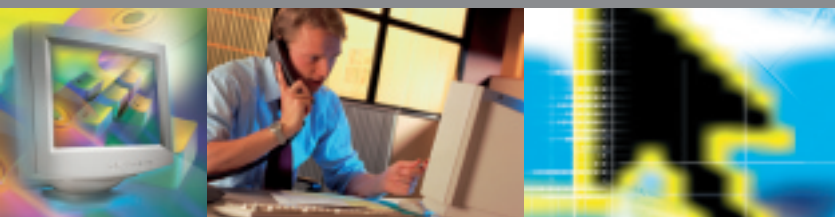


Secure Electronic Banking at ABN AMRO



OfficeNet



Secure Electronic Banking at ABN AMRO

1 Introduction

You are, or you are about to become a user of one of ABN AMRO Bank's Electronic Banking products. ABN AMRO has developed and tested this product with great care, in conjunction with specialists and users.

The security of its Electronic Banking products has a high priority at ABN AMRO and ABN AMRO has made every effort to ensure that your electronic banking transactions are secure. Nevertheless, you may run a number of risks over which ABN AMRO has no control. These guidelines provide you with a number of tips that can help you avoid these risks as much as possible. However, it is your responsibility to ensure that you act in accordance with these guidelines at all times.

Section 2 describes the risks that you may incur and the possible consequences. Section 3 explains the efforts ABN AMRO has undertaken to enhance security. Section 4 is the most important section, describing the measures you can take to improve security. Section 5 contains the conclusion and Section 6 a glossary.

If you have any comments with regard to shortcomings that you have identified in these guidelines, the security of the software, or if you have general suggestions for the improvement of security or the information provided, please let us know. We shall investigate your suggestions and make the necessary improvements where possible. You will always be able to find the latest version of these guidelines at <http://www.abnamro.nl/safety>.

2 Risks

What risks do you run?

With both your accounting software and your Electronic Banking software, you run the risk of the software being misused. Two types of risks can be distinguished: organisational and computer risks.

Organisational risks are caused by the insufficient restriction of authorisations within your internal organisation with regard to the use of Electronic Banking software. Computer risks result from the open character of a computer, e.g. your computer could become contaminated with a virus or certain people can gain unauthorised access to your data. In a properly secured environment, both organisational and computer risks are limited or have been eliminated completely.

There are two potential consequences of misuse of your software:

- *Fraud*
In the case of fraud, data in your software has been changed, ultimately allowing unauthorised transactions to be sent to the bank.
- *Invasion of privacy*
An invasion of privacy means that unwanted third parties can view your transactions (sent or still pending), reports (statements) or your current financial status.

The possible consequences.

Some of the actions that may be carried out with your Electronic Banking software by unauthorised persons are outlined in the following subsections. Subsections 1 through 4 describe the required resources, secret passwords or codes that an unauthorised person would have to have or be aware of.

The possible consequences of each action are listed as either: invasion of privacy, fraud or both.

The assumption underlying the following overview is that the authorisation of users is **not** restricted in your software or your Electronic Banking contract.

1 Use of the Electronic Banking software password

With the Electronic Banking software password (and the accompanying user ID), one can:

- view reports (privacy);
- create transactions (fraud);
- export report data (privacy/fraud).

2 Use of Calculator + bank password + Electronic Banking software password

Anyone who has your Electronic Banking software password, your calculator and your bank password can:

- do everything listed in Subsection 1;
- retrieve reports from the bank server during a communication session (privacy);
- authorise and send transactions (fraud).

3 Use of Smartcard + PIN + Electronic Banking software password

Anyone who has your Electronic Banking software password, Smartcard and the accompanying PIN can:

- do everything listed in Subsection 1;
- authorise transactions (fraud).

4 Use of Smartcard + PIN + bank password + Electronic Banking software password

Anyone who has your Electronic Banking software password, bank password, Smartcard and the accompanying PIN can:

- do everything listed in Subsection 1;
- retrieve reports from the bank server in a communication session (privacy);
- authorise transactions (fraud);
- send transactions (fraud).

5 Computer environment with insufficient security

Anyone with access to your computer can perform actions including the following:

- altering files (fraud);
- damaging files (fraud);
- viewing files and data (privacy);
- copying files and data (privacy/fraud).

In the first two cases, files and/or programmes may no longer work properly (and safely). In the latter two cases, files or data may fall into the hands of unauthorised persons.

6 Organisational environment with insufficient security

Depending on the authorisations and knowledge of the people within your immediate environment, the consequences as listed in Items 1 to 5 could occur.

3 What ABN AMRO does to enhance security

ABN AMRO has taken many different measures to make electronic banking as safe as possible for you. A summary is set out below:

1 Both knowledge and possession are necessary

Both knowledge and possession are needed for electronic banking at ABN AMRO:

- possession: A security token (Calculator or Smartcard) is required;
- knowledge: A bank password is required;
- knowledge: An Electronic Banking software password is required;
- knowledge: A PIN is required for the use of a Smartcard.

2 The ABN AMRO bank server is secured

- the ABN AMRO bank server itself is secured;
- data transmission between your software and the ABN AMRO bank server is secured.

3 Your Electronic Banking Software is secured

- a software password is needed (or can be set) to gain access to the Electronic Banking software;
- the Electronic Banking software detects changes in your transaction data that have been made from outside the software;
- reports in your Electronic Banking software are scrambled (or this can be set).

4 User authorisation can be restricted

User authorisations can be restricted in two ways:

- by configuring your Electronic Banking software;
- in the Electronic Banking contract.

See Section 4 for details of these possibilities.

4 What you can do to control the risks

In addition to the measures that ABN AMRO has already taken, you should also take certain precautions to ensure safe electronic banking. Some of the measures that can be implemented, depending on your situation, are described below.

1 Make one person responsible for security measures:

For the secure use of your Electronic Banking software, we advise you to appoint only one person who will be responsible for all security measures. This person (often it will be you) is referred to in these guidelines as the Main User. The Main User can change and set all authorisations within your Electronic Banking software.

The Main User:

- supervises the correct installation of the software in accordance with the instructions;
- supervises safe storage of the installation software (to prevent unauthorised use);
- after the installation, the first to start up the software is the person with ultimate responsibility and therefore is automatically assigned all authorisations;
- assigns authorisations to the users in the software ;
- supervises the correct use and management of the security tokens;
- supervises the correct recording of the accounts and security tokens in the software ;
- provides the installation of any new versions of your Electronic Banking software.

2 Divide the functions within your organisation

In addition to the above mentioned function of Main User you can also distinguish between a number of other functions within your organisation:

- *Data entry function*
This function involves entry of transactions for payment. Authorisation and sending transactions is not possible. No security token is required for this function.
- *Authorisation function*
This involves authorising payment transactions that have already been entered into the system. This function requires a security token.
- *Send function*
After the user with the authorisation function has authorised the transactions, the user with the send function can send them to the bank.

If a Calculator is used as a security token, the authorisation function and the send function are combined.

3 Appoint different contacts for security tokens, PINs and bank passwords:

To ensure that all of a user's details never fall into the hands of one and the same person, you can designate two different contact persons in the Electronic Banking contract: a contact for safety measures and a contact for password. ABN AMRO can then initiate separate dispatches of security tokens and PINs/bank password letters in its administration. You are advised to make use of this option.

The contact for safety measures receives and manages the security tokens, and keeps a record of which security token has been issued to each individual user. The Main User would be an excellent choice for this task.

The contact for password will receive the relevant information from the bank through mail. Given the confidential nature of this information, this contact person should check that the letters are still properly sealed upon receipt and that they have not been tampered with. Never issue damaged envelopes containing a password or PIN to a user. In the event that an envelope is in fact damaged, the contact person should immediately contact the ABN AMRO Service Desk. The Service Desk will arrange to send a new PIN and/or password. The contact person must always issue letters containing PINs to the user unopened. The contact person should however, open the password letters as they contain the bank passwords for all users. The contact for password should notify the users of these bank passwords. The passwords should be changed immediately after they have been used for the first time. The software will automatically instruct the user to do so.

4 Treat your security token(s) with care

ABN AMRO issues security tokens to your company/organisation. The security tokens that have been issued are recorded in ABN AMRO's contract administration records by user serial number.

In your software, you administrate the user serial numbers used by the various users within your organisation. The bank passwords are then sent to the contact for password for each user serial number.

To ensure that due care is taken in respect of the security tokens, you are advised:

- to personalise each security token that has been issued, record which security token has been issued to each individual user;
- to issue written instructions to users relating to the care of the security token. Users should sign a copy of the instructions to show they have read them. The instructions should contain points for attention on matters including keeping the token in a safe place, the storage method that should be used, the fact that it should never be lent to anyone, etc. You will find an example of such instructions attached as an appendix to this document. An electronic version of this document is available at <http://www.abnamro.nl/safety>.

5 Never disclose your bank password, PIN or Electronic Banking software password

Users must comply with the following requirements in respect of bank passwords and PINs:

- bank passwords and PINs must never be written down;
- passwords must be changed regularly;
- the bank password must always differ from the Electronic Banking software password;
- due care should be taken when keying in passwords and/or PINs, to ensure that they cannot be seen by others.

You are advised to comply with these rules in respect of passwords used to gain access to the PC and the network as well.

6 Monitor your computer environment

A computer, in a network or otherwise, is not secure if you fail to take adequate measures. Unauthorised parties can gain access to your computer through the Internet, your network or directly from your computer. You will have to determine which extra measures should be taken to enhance the security of your financial traffic to and from the bank.

The following measures can be taken to protect your computer environment:

- Always log off when you (temporarily) finish working on your computer. This will allow you to protect your computer against unauthorised use.
- Use an anti-virus program and ensure that you always install the latest updates thereof. Ensure that the anti-virus program is always active, even when you are not connected to the Internet. Do a full scan of your computer with the anti-virus program at fixed times (e.g. twice a month). Follow your software provider's recommendations.
- Security errors are often found in Internet browsers. Always check whether or not you have the latest version of your browser. Repair programs or new versions of browsers are provided regularly.
- To prevent hacking, it is advisable to make use of a firewall (software that checks the interface between your computer and the Internet) when you are using the Internet.
- You are advised to change passwords regularly and to avoid combinations that can be guessed easily.
- Only use software if you know its origin and are familiar with it. It is ABN AMRO's policy to never distribute programs through e-mail or news groups.

7 Configure the software in accordance with your security requirements

Depending on the software that you use, you can decide whether or not to set access levels for the users of certain functions. You can assign specific rights and authorisations for each user. The possibilities vary from application to application. Examples of such possibilities include:

- signing transactions (possibly with a maximum limit, individually or together with another user);
- viewing reports;
- creating transactions;
- exporting/deleting transaction files;
- importing transaction files;
- sending via the bank for additional authorisation;
- screen procurement (setting user access for each screen).

At <http://www.abnamro.nl/safety> you will find a document which describes the options provided by the different applications. You can also consult the helptext and/or the manual for your software.

8 Restrict user authorisations through the Electronic Banking contract

You can also restrict the authorisations of the security tokens that have been issued to your users in the Electronic Banking contract. Remember that user authorisations cannot be changed as quickly and flexible in the contract as they can in the software. If you want to change authorisations in the contract, an amendment of the contract will be necessary.

Each user that is included in the Electronic Banking contract always has one of the following options:

- *Authority Alone with communication*
The user may sign and send transactions and/or retrieve account information independently.
- *Authority Not with Communication*
The user may not sign payment transactions, but may send them to the bank and retrieve account information.
- *Authority Together with communication*
The user may only sign transactions together with another user, but may send instructions and/or retrieve account information independently.
- *Authority Alone without communication*
The user may sign payment transactions, but may not send them to the bank.
- *Authority Together without communication*
The user may only sign payment transactions together with another user but may not send them to the bank.

NOTE *Authorisations for Authority together with communication, Authority alone without communication, and Authority together without communication are only possible with the use of a Smartcard and OfficeNet Extra.*

9 Destination accounts

The destination accounts function enables you to stipulate a limited number of counter-party accounts ('destination accounts') in a single contract. If payment instructions are received, the bank will only process these if the counter-party's account is shown to be a destination account.

10 Restrict the possibilities for issuing payment and/or securities transactions in your Electronic Banking contract

You can state in the Electronic Banking contract where and when payment and/or securities transactions may be submitted against a particular account (securities transactions are only possible in combination with HomeNet and OfficeNet Plus). This can only be set for all users.

11 Remove users who are no longer needed

Users that are no longer required can be removed from the Electronic Banking software. You can do this for redundant user numbers and the accompanying security tokens. The latter requires an amendment of the Electronic Banking contract.

5 Conclusion

With these guidelines and the possibilities in your software, ABN AMRO is doing its best to support you in the usage of secure Electronic Banking. However, it is important for you to remember that you too must make the required effort in this regard.

6 Glossary

Bank password

The bank password is required for successful communication with the bank server. This form of communication is only possible if a Calculator or a Smartcard (including the accompanying PIN) is available.

Security token

Two security tokens can be used for ABN AMRO Electronic Banking: the Calculator and the Smartcard.

Calculator

The Calculator is used to communicate with the bank. You will also need the accompanying bank password.

Computer environment

The computer environment refers to your own computer (including the software installed on it) as well as any network and/or Internet connection.

Organisational environment

The organisational environment refers to all the people in your environment (on a day-to-day basis). This includes people who share your home or office, or who are your employees. These people could have permission to perform certain activities within your environment. These could include:

- someone who shares your home and with whom you share a computer (and possibly the Electronic Banking software);
- a colleague who has permission to use your Electronic Banking software .

Electronic Banking Software password

The Electronic Banking software password is needed to gain access to the Electronic Banking software.

Smartcard

The Smartcard is used to communicate with the bank. However, you also require the accompanying PIN and the bank password. In addition, the Smartcard and PIN are also used to authorise ('sign') transactions.

Confirmation of receipt of security token

name:

hereby declares that he/she has taken receipt of:

Smartcard / Calculator ¹

Number of security token:

For contract number:

User serial number:

**Particulars
of security
token**

The undersigned declares that the security token will be treated with due care, which includes the following:

- The security token is stored in a safe place when not in use.
- The PIN is never written down.
- The PIN is never disclosed.
- The security token is never lent to another person.

Place:

Signature:

¹ Delete whichever does not apply.